REMARKS

Claims 1-28 are pending in the application. Claims 1-28 are rejected under 35 U.S.C. § 103. Claims 1 and 15 are amended herein. No new matter is added.

Telephone Conversation With Examiner

Examiner Perungavoor is thanked for the telephone conversation conducted on June 9, 2008. Proposed claims amendments were discussed. No agreements were reached.

Initial Matters

On page 2, the Office Action provides the standard form paragraph regarding an obviousness rejection under 35 U.S.C. 103(a). However, the heading for the rejection recites "Claims 1-2, 7-9, 24-26 are rejected under 35 U.S.C. 102(b) as being anticipated" which provides some confusion as to the intention of the Office Action. Clarification on the record is respectfully requested. Applicant's Representative will assume in the following response that the rejections set forth in the Office Action are based in 35 U.S.C. 103(a) and are based upon obviousness, not anticipation, of the enumerated claims.

Regarding the Rejections under 35 U.S.C. §103

Claims 1-2, 7-9, and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over "RFC-3244-Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols", Swift et al (hereinafter "Swift") in view of Puthiyandyil et al. (US Patent 6,950,862, hereinafter "Puthiyandyil"). Claims 3-6, 10-13, 15-18, 21-23, and 27-28 are rejected in view of Swift, Puthiyandyil and further in view of "rpcsec_gss, kadmin service principal, etc" (hereinafter "Coffman"). These rejections are respectfully traversed.

Swift, Puthiyandyil, and Coffman, whether considered separately or in any combination, neither disclose nor suggest "sending a subsession key to the client computer, wherein the subsession key may be used by the client computer to switch from a first encryption to a second encryption algorithm for use in conjunction with the selected encryption algorithm to encrypt future communications to the server computer" as recited in

claims 1, 8, and 24; "switching to the specified encryption algorithm if the subsession key for use with the specified encryption algorithm is delivered" as recited in claim 8; of "means for switching to one or more of said one or more encryption algorithms for the purpose of subsequent communications with said first computer." as recited in claim 24.

Swift is directed to the process of specifying, setting, and resetting passwords within the Windows 2000 implementation of the Kerberos change password protocol that interoperates with the original Kerberos change password protocol. Puthiyandyil is directed to computational service offloading, such as compression and encryption offloading, across point-to-point communication links. Coffman is directed to the use of the GSS API in the specification of Kerberos protocol based systems.

The claimed subject matter relates to encryption algorithm negotiation in the context of encryption-based authentication protocols. The claimed subject matter has the added benefit of providing a system and method that need not interfere with the standard operation of existing authentication protocols. A first computer sends a negotiation request to a second computer in which the negotiation request specifies that the first computer supports a selected encryption algorithm. The second computer may return a subsession key for encryption using the selected encryption algorithm. Both first and second computers may then switch to encryption in the selected encryption algorithm, using the subsession key to encrypt future communications.

As previously stated, regarding claims 1, 8, and 24, claim 1 recites, in part, "sending a subsession key to the client computer, wherein the subsession key may be used by the client computer to switch from a first encryption to a second encryption algorithm for use in conjunction with the selected encryption algorithm to encrypt future communications to the server computer" and claim 8 recites in part, "switching to the specified encryption algorithm if the subsession key for use with the specified encryption algorithm is delivered" and claim 24 recites in part, "means for switching to one or more of said one or more encryption algorithms for the purpose of subsequent communications with said first computer." The Office Action admits on Page 2 that the Swift reference does not teach or disclose the

negotiating of encryption algorithms. In addition, however, the Swift reference also does not teach or disclose "switching to the specified encryption algorithm" in any form, which is recited in part in claims 1, 8 and 24.

It is submitted Swift has been mis-characterized. The Office Action asserts that the Swift reference discloses or teaches "switching to the specified encryption algorithm if the subsession key is delivered" on page 3 of the reference, however, Swift does not. Swift on page 3 discloses the process for changing a password after an authenticated password has been generated and a subsession key has already been assigned. In fact, on page 2 of the Swift reference the AP-REQ message that is sent from the first (client) computer to the second (server) computer must already contain a previously generated subsession key (see Swift, Page 2, "The authenticator in the AP-REQ must include a subsession key"). There is no "specification of encryption" of any kind in the Swift reference, and the only mention of encryption is that an encryption algorithm is used to decrypt the password from the first (client) computer. Thus, Swift is completely silent as to "switching to the specified encryption algorithm".

The Office Action looks to Puthiyandyil to remedy this lack of teaching; however, Puthiyandyil does not cure the deficiencies of Swift. Puthiyandyil discloses, in Figure 9, only that the encryption *parameters* (emphasis added) are passed in a negotiation message from a first computer to a second computer. The encryption parameters are passed and negotiated to be certain that the methodology of encryption is consistent between the two computer systems. If the encryption methodology is not consistent, there is no disclosure of the two computer systems negotiating to utilize a different encryption algorithm or methodology. Therefore, Puthiyandyil does not disclose either "switching to the specified encryption algorithm" or "receiving" or "sending a negotiation request" wherein the negotiation request "specifies and encryption algorithm for subsequent communication" as recited in claims 1, 8 and 24. Thus, the combination of Swift and Puthiyandyil does not provide the teaching to render at least this feature of claims 1, 8 and 24 obvious.

With regard to the "including a negotiation request with an authentication protocol process communication from the first computer to the second computer, wherein the negotiation request specifies that the first computer supports one or more encryption

algorithms" recitation in claim 15, this claim is rejected the Office Action admits on page 5 that the combination of Swift and Coffman does not disclose this limitation and looks to Puthiyandyil to remedy this lack, however, it does not.

Once again, Puthiyandyil discloses in Figure 9 only that the encryption *parameters* (emphasis added) are passed in a negotiation message from a first computer to a second computer. There is no disclosure of the two computer systems negotiating to utilize a different encryption algorithm or methodology. Thus, Puthiyandyil does not disclose "including a negotiation request with an authentication protocol process communication from the first computer to the second computer, wherein the negotiation request specifies that the first computer supports one or more encryption algorithms" as recited in claim 15. Therefore, the combination of Swift, Coffman, and Puthiyandyil does not provide the disclosure to render the claim obvious. Reconsideration and allowance are respectfully requested.

Claims 2-7, 9-14, 16-23, and 25-28 all depend, either directly or indirectly, from one of claims 1, 8, 15, and 24. As such, the applicants submit that these claims are patentable over the combination of Swift, Coffman and Puthiyandyil for at least the same reasons as stated above with respect to claims 1, 8, 15 and 24. Accordingly, reconsideration and allowance are respectfully requested.

Further, a *prima facie* case of obviousness has not been established because support for obviousness comprises only conclusory statements. A *prima facie* case of obviousness has not been established because it has not been explained why one of skill in the art at the time of the claimed subject matter would have been motivated to combine Swift and Puthiyandyil. And, it has not been explained how Swift and Puthiyandyil would be combined to arrive at the claimed subject matter.

The MPEP provides several guidelines for rejecting a claim under 35 U.S.C. 103(a). Specifically, reference is made to MPEP § 2141. III - Rationales To Support Rejections Under 35 U.S.C. 103, which states in part:

> "Office personnel must explain why the differences(s) between the prior art and the claimed invention would have been obvious to one

> of ordinary skill in the art. ... The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR* noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Court quoting *In re Kahn,* 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006), stated that "'[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'" *KSR*, 550 U.S. at ___, 82 USPQ2d at 1396." (Emphasis added)

Additionally, the Examiner should explain how to combine the references, per MPEP 706.02(j).

> "35 U.S.C. 103 authorizes a rejection where, to meet the claim, it is necessary to modify a single reference or to combine it with one or more other references. After indicating that the rejection is under 35 U.S.C. 103, the examiner should set forth in the Office action: (A) the relevant teachings of the prior art relied upon, preferably with reference to the relevant column or page number(s) and line number(s) where appropriate, (B) the difference or differences in the claim over the applied reference(s), (C) the proposed modification of the applied reference(s) necessary to arrive at the claimed subject matter, and (D) an explanation >as to< why >the claimed invention would have been obvious to< one of ordinary skill in the art at the time the invention was made**." (Emphasis added)

Further, when explaining how to modify a reference, "the proposed modification can not render the prior art unsatisfactory for its intended purpose" (MPEP 2143.01.V), and "the proposed modification can not change the principle of operation of a reference. (MPEP 2143.01.VI).

CONCLUSION

For the forgoing reasons, it is respectfully submitted that the instant application is in condition for allowance. Reconsideration and early allowance is hereby respectfully requested.

Date: June 11, 2008

/Joseph F. Oriti/
Joseph F. Oriti
Registration No. 47,835

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439